

Web Application Firewall

Модуль «Web Application Firewall» (WAF) расположен в Меню «Защита». Данный модуль отслеживает и блокирует весь HTTP/HTTPS трафик входящий и исходящий от установленных Web-приложений на «ИКС» или в локальной сети. Путём анализа HTTP/HTTPS трафика WAF может предотвращать атаки, основанные на недостатках защиты Web-приложений, таких как: SQL инъекции, межсайтовый скрипting (XSS), включение файлов, не правильная настройка безопасности.

The screenshot shows a log viewer for the Web Application Firewall. At the top, there's a header bar with 'ИКС > Web Application Firewall' on the left, 'Администратор' in the center, and a message '17' with an envelope icon on the right. Below the header are navigation buttons for date ranges ('13.09.2019 - 13.09.2019', 'Сегодня', 'Неделя', 'Месяц', 'Другой период'), an 'Экспорт' button (blue background with white text), a 'Удалить логи' button, a search bar ('Поиск...'), and a magnifying glass icon. The main area displays a list of log entries. Each entry contains a timestamp (e.g., '12:36:57'), a source IP ('192.168.17.8'), a date ('[13/Sep/2019:12:36:57 +0300]'), a method ('GET'), a URL ('/styles.css?ver=7.0.0'), a status code ('200'), a file size ('129812'), and a user agent ('Mozilla/5.0 (Windows NT 6.1; rv:70.0) Gecko/20100101 Firefox/70.0'). The log entries are color-coded: white for standard system messages, green for inclusion/exclusion, yellow for warnings, and red for errors. On the right side of the log list, there are scroll controls (up and down arrows). At the bottom, there are page navigation buttons ('<<', '<', 'Стр', '1', 'из 1', '>', '>>') and a text 'Показаны записи 1 - 84 из 84'.

В самом модуле отображается сводка всех системных сообщений модуля с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение) - зеленым, предупреждения - желтым, ошибки - красным. В правом верхнем углу модуля находится строка поиска. А также возможность выбора периода отображения журнала событий. По умолчанию журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

Для включения/выключения фильтрации трафика необходимо установить/снять соответствующий флажок при добавлении или редактировании «**Виртуального хоста**»/«**Виртуального хоста с перенаправлением**», расположенных в Меню «**Файловый сервер**» - «**Веб**» - вкладка «**Веб-ресурсы**». Стоит отметить, что **Веб-сервер** должен быть настроен и запущен.

From:
<https://doc-old.a-real.ru/> - **Документация**



Permanent link:
<https://doc-old.a-real.ru/doku.php?id=ics70:waf&rev=1573397216>

Last update: **2020/01/27 16:28**